UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/621,148	07/16/2003	Oleg Ivanov	MS1-1594US	1195

22801 7590 11/28/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
KENDALL, CHUCK O	

ART UNIT	PAPER NUMBER
2192	

MAIL DATE	DELIVERY MODE
11/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/621,148	IVANOV ET AL.	
	Examiner	Art Unit	
	Chuck O. Kendall	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-13,16-20,22-25,27,28 and 33* is/are pending in the application.

4a) Of the above claim(s) *4,5,14,15,21,26,29-362* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-13,16-20,22-25,27,28 and 33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

1. This in response to arguments/amendments filed 09/21/07.

2. Claims 1 – 3, 6 –13,16 – 20, 23 – 25, 27, 28 and 33 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 3, 6 –13,16 – 18, 20, 23 – 25, 27, 28 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Donohue USPN 6,199,204 B1 in view of Banzhof US 7,000,247 B2.

Regarding claim 1, Donohue discloses a processor-readable medium comprising processor-executable instructions configured for:

receiving a binary signature (8:45 – 50, shows downloading file which contains a digital signature, 10:50 – 65, also discloses that the code is machine readable code, i.e. binary code);

receiving a security patch (4:23 – 27, see patch and downloaded);

identifying a vulnerable binary file on a computer based on the binary signature (8:45 – 60, see retrieved file160 is analyzed 240 based on digital signature); and

updating the vulnerable binary file on the computer with the security patch (7:60 – 62 and 5:7 – 12, see modifying existing program and patch and see error correction for vulnerable binary file).

Although Donohue doesn't expressly disclose receiving the binary signature at the server computing device as well as the security patch and identifying from the server device the vulnerable binary file and then updating from the server device the vulnerable file on the client, Donohue does however disclose an updater component on a network which updates the file other computers on the network (i.e. client) and checks the digital signatures to verify it authenticity (8:45 – 60). Banzhof in an analogous art and similar configuration of vulnerability resolution discloses receiving binary signatures, identifying the vulnerable files (FIG. 5a – FIG 5b and all associated text, also see (2:5 – 10). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Donohue and Banzhof because "downloaded signatures may then be used to address or resolve vulnerabilities on client machines having security vulnerabilities" (Banzhof, 2:10 – 12).

Regarding claim 2, a processor-readable medium as recited in claim 1, wherein the identifying a vulnerable binary file located on a client computing device includes comparing a bit pattern of the binary signature against binary files located on the computer, the bit pattern associated with a security vulnerability (6:35 – 37, shows

updater file is a binary file and 8:50 – 9:7, shows comparisons between product identifier and release number of retrieved file).

Regarding claim 3, a processor-readable medium as recited in claim 1, wherein the updating the vulnerable binary file on the computer includes installing the security patch on the computer (8:7 – 12, see modifying existing program and patch code).

Regarding claim 6, a processor-readable medium as recited in claim 1, wherein the computer is a client computer and the receiving includes receiving the binary signature and the security patch from a distribution server configured to distribute to the client computer, binary signatures that identify vulnerable files and security patches configured to fix the vulnerable files (7:55 – 65, see server and patches and see 8:10 – 15, for error correction).

Regarding 7, a server comprising the processor-readable medium as recited in claim 1, (7:55 – 65, see server).

Regarding claim 8, Donohue anticipates a processor-readable medium comprising processor-executable instructions configured for:

receiving a binary signature that identifies a security vulnerability in a binary file (8:45 – 50, shows downloading file which contains a digital signature, 10:50 – 65, also discloses that the code is machine readable code, i.e. binary code);

receiving a security patch configured to fix the security vulnerability in the binary file (4:23 – 27, see patch and downloaded); and

distributing the binary signature and the security patch to a plurality of servers (7:60 – 62 and 5:7 – 12, see modifying existing program and patch and see error correction for vulnerable binary file, also see 7:55 – 65, server).

Regarding claim 9, a processor-readable medium as recited in claim 8, wherein the distributing includes:

sending a notice to each of the plurality of servers regarding the security vulnerability and the available patch (13:15 – 20);

receiving a request to send the binary signature and the security patch (13:6 – 10); and

sending the binary signature and the security patch in response to the request (13:5 – 9, see complete update also see 6:6 – 10, see downloading from another computer).

Regarding claim 10, a distribution server comprising the processor-readable medium as recited in claim 8 (7:55 – 65, see server).

Regarding claim 11, Donohue anticipates a processor-readable medium comprising processor-executable instructions configured for:

receiving a binary signature from a server (8:45 – 53, shows the digital signature is analyzed when file is retrieved);

searching for the binary signature in binary files (8:10 – 20 and 45 – 57);

sending a request to the server for a security patch if a binary file is found that includes the binary signature (13:6 – 10);

receiving the security patch from the server (4:23 – 27, see patch and downloaded); and

updating the binary file with the security patch (7:60 – 62 and 5:7 – 12, see modifying existing program and patch and see error correction for vulnerable binary file, also see 7:55 – 65, server).

Regarding claim 12, a client computer comprising the processor-readable medium as recited in claim 11, see reasoning above in claim 11 and for client see (8:18 – 20, local computer 10).

Regarding claim 13, Donohue discloses a method comprising:

receiving a binary signature (8:45 – 50, shows downloading file which contains a digital signature, 10:50 – 65, also discloses that the code is machine readable code, i.e. binary code);

searching for a vulnerable file based on the binary signature (8:45 – 57);

if a vulnerable file is found, requesting a security patch (8:10 – 14); and

fixing the vulnerable file with the security patch (8:10 – 20 and 45 – 57).

Although Donohue doesn't expressly disclose receiving the binary signature at the server computing device as well as the security patch and identifying from the server device the vulnerable binary file and then updating from the server device the vulnerable file on the client, Donohue does however disclose an updater component on a network which updates the file other computers on the network (i.e. client) and checks the digital signatures to verify it authenticity (8:45 – 60). Banzhof in an analogous art and similar configuration of vulnerability resolution discloses receiving binary signatures, identifying the vulnerable files (FIG. 5a – FIG 5b and all associated text, also see (2:5 – 10). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Donohue and Banzhof because "downloaded signatures may then be used to address or resolve vulnerabilities on client machines having security vulnerabilities" (Banzhof, 2:10 – 12).

Regarding claim 16, a method as recited in claim 13, wherein the fixing includes installing the security patch on the client computer (7:43 – 45, shows the installation process).

Regarding claim 17, a method as recited in claim 13, wherein the searching includes comparing the binary signature to binary information on a storage medium of the client computer (6:35 – 37, shows updater file is a binary file and 8:50 – 9:7, shows comparisons between product identifier and release number of retrieved file also see

6:7 – 10 for storage medium).

Regarding claim 18 and 27, a method/computer as recited in claim 17, wherein the binary information is selected from the group comprising:

an operating system (6:7 – 10, shows a local computer system, hence an OS is inherent);

an application program file (3:60 – 63, see installed computer programs);

and a data file (3:60 – 63, see software update).

Regarding claim 20, which recites similarly to claim 13, see rationale as previously address above.

Regarding claim 23, the computer version of claim 11, see rationale as previously addressed above.

Regarding claim 24, the server version of claim 11, see rationale as previously addressed above.

Regarding claim 25, the computer version of claim 13, see rationale as previously addressed above.

Regarding claim 28, the computer version of claim 1, see rationale as previously addressed above.

Regarding claim 29, the computer version of claim 6, see rationale as previously addressed above.

Regarding claim 30, Donohue anticipates a distribution server comprising:

a database (FIG.1, 40 and all associated text); and

a distribution module configured to receive a binary signature and a security patch, store the binary signature and the security patch in the database, and distribute the binary signature and the security patch to a plurality of servers (8:45 – 60, see retrieved file160 is analyzed 240 based on digital signature also see 7:60 – 62 and 5:7 – 12, see modifying existing program and patch and see error correction for vulnerable binary file, also see 7:55 – 65, server).

Regarding claim 31, a distribution server as, recited in claim 30, wherein the distribution module is further configured to receive a request from a server for the binary signature and the security patch and to distribute the binary signature and the security patch to the server in response to the request (8:45 – 60, see retrieved file160 is analyzed 240 based on digital signature).

Regarding claim 32, the server version of claim 11, see rationale as previously addressed above.

Regarding claim 33, a server as recited in claim 32, further comprising:

a database (FIG.1, 40 and all associated text); and

the scan module further configured to receive the binary signature and the security patch from a distribution server and to store the binary signature and the security patch in the database (8:45 – 60, see analyzed 240 and digital signature).

5. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Donohue USPN 6,199,204 B1 in view of Banzhof US 7,000,247 B2 as applied in claim 17 in view of Gabel 5,930,504.

Regarding claim 19, Donohue as modified discloses all the claimed limitations as applied in claim 17 above including:

A hard disk (6:1 – 10, see system memory), a magnetic floppy disk (6:1 – 10, see diskette), an optical disk (6:7 – 10, see CD) and a

network-attached storage (6:18 – 20, see repository).

Donohue as modified by Banhof doesn't expressly disclose a flash memory card and an electrically erasable programmable read-only memory. However Gabel in an analogous art and similar configuration of updating/patching software discloses the use of electrically erasable programmable read only memory (flash EEPROM) and states

that use of "flash memory permits non-invasive updating procedures so that the nonvolatile memory can be updated from an update file" (1:60 – 65). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Donohue, and Banzhof with and Gabel because, it would enable updating from an update file.

Response to Arguments

6. Applicant's arguments filed 09/21/07 have been fully considered but they are not persuasive.

Argument (1), Applicant argues on page 14 of his response that, Donohue in view Banhof doesn't teach or suggest the recited limitation of "receiving a binary signature", "receiving a security patch" and "identifying a vulnerable file", as well as not teaching" updating from the server computing device, the vulnerable binary file located on the client computing device".

Response (1), Examiner disagrees, in Banhof FIG. 5a, 82 and associated text specifically in 8:60 – 67, Banhof teaches downloading available signatures (remediation signature) and vulnerability information. Banhof also in 5:25 – 30 discloses downloading this information to a client server 22 from the flash server. Banhof further discloses that a remediation signature may also include a patch or an update where it can also be download to cure the vulnerabilities. Although Donohue doesn't expressly teach downloading the signatures, he does however disclose downloading the patch information to a local system, which may be delivered from another device in the

network, and Examiner interprets this to also encompass and client server connection, which Applicant argues doesn't exist in Donohue, from his arguments on page 14, last paragraph.

Argument (2), Applicant in claim 11, also argues that neither Donohue nor Banzhof shows "sending a request from the client computer to the server for a security paftch if a binary file is found that includes the binary signature".

Response (2), Examiner disagrees, In Banzhof it is disclosed in 9:25 – 40, that a user can select particular clients to receive the remediation signatures and a notification can be sent out.

Regarding all other arguments not discussed, are merely modifications of the previous arguments already discussed above.

Correspondence information

7.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chuck Kendall whose telephone number is 571-272-3698. The examiner can normally be reached on 10:00 am - 6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Dam can be reached on 571-272-3695. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ck.

TODD INGBERG
PRIMARY EXAMINER